

Tozzini Freire.

ADVOGADOS

BOLETIM
CYBERNEWS.

27ª Edição | 2023



Sumário

01

4

02

10

03

12

04

17

05

18

06

20

01

Contexto Brasileiro.

ANPD esclarece sobre a atuação do Encarregado e emissão de selos de conformidade com a LGPD

Em 31 de março de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) publicou esclarecimentos a fim de mitigar a disseminação de informações enganosas sobre suas supostas exigências.

Dentre eles, destacamos que a ANPD:

- ainda não estabeleceu normas complementares sobre as atribuições do encarregado, que serão objeto de regulamentação futura;
- não reconheceu oficialmente a validade de qualquer norma ou guia com orientações sobre a atuação do encarregado;
- não credencia empresas ou entidades para a emissão de selos que atestem a conformidade à Lei Geral de Proteção de Dados (LGPD).

Além disso, a ANPD esclareceu que o encarregado pode se relacionar diretamente com ela e com os titulares de dados, sem necessidade de intermediação por quaisquer entidades. Além disso, não há qualquer exigência legal de registro de profissionais de proteção de dados ou de encarregados perante a ANPD ou associações privadas.

Novas diretrizes sobre a elaboração do relatório de proteção de dados são emitidas pela ANPD

Com o objetivo de fornecer mais esclarecimentos à sociedade sobre a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), a ANPD publicou um documento e infográficos de perguntas e respostas sobre o tema. Entre as recomendações, são tratadas sobre sua elaboração, as metodologias a serem consideradas pelos controladores para a gestão de riscos e os requisitos mínimos.

Dentre as diversas orientações, a ANPD recomenda que a elaboração do RIPD aconteça antes do tratamento de dados; estabelece as diretrizes que devem ser consideradas na análise de gestão de riscos; e identifica o que pode ser considerado como “alto risco” para fins de elaboração do relatório.

Vale frisar que a elaboração do RIPD constitui uma obrigação legal do controlador (art. 5º, XVII, e 38, LGPD). Além disso, a ANPD pode solicitá-lo, especialmente, para controladores em geral, quanto às suas operações de tratamento, incluindo as que envolvam dados pessoais sensíveis (art. 38, LGPD), e quando o tratamento de dados tiver o legítimo interesse como fundamento (art. 10, §3º, LGPD).

Quando solicitado, esse documento deve conter a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados. Isto é, deve conter, ao menos, a:

- descrição dos tipos de dados pessoais tratados;
- metodologia usada para o tratamento e para a garantia da segurança das informações; e
- análise do controlador com relação às medidas, salvaguardas e aos mecanismos de mitigação de riscos adotados.



BCB e bureaus de crédito assinam acordo para compartilhamento de informações

O Banco Central do Brasil (BCB) assinou, no final de março, um Acordo de Cooperação Técnica (ACT) com cinco gestores de bancos de dados, os chamados “bureaus de crédito”. O ACT visa dar efetividade à Resolução do Conselho Monetário Nacional (CMN) nº 5.037/22, que dispõe sobre o acesso ao Sistema de Informações de Créditos (SCR).

Os cinco bureaus de crédito que firmaram o acordo com o BCB foram: Boa Vista Serviços S.A., Confederação Nacional de Dirigentes Lojistas (CNDL - SPC Brasil), Gestora de Inteligência de Crédito S.A. (Quod), Serasa S.A. e TransUnion Brasil Sistemas em Informática Ltda.

A partir da assinatura, tanto o Banco Central quanto as empresas se beneficiam. De um lado, estas irão compartilhar dados de interesse do BCB, como notas de crédito (scores) e histórico de crédito não bancário. Do outro lado, o BCB poderá permitir o acesso dos bureaus ao SCR.

O acordo previu, ainda, itens que objetivam proteger a privacidade e a proteção dos dados de titulares, como o comprometimento com a confidencialidade de informações sensíveis e fluxo de contestação caso não se concorde com algum dado.



02

Poder Judiciário.

Superior Tribunal de Justiça publica Política de Proteção de Dados

A Resolução do Superior Tribunal de Justiça (STJ/GP5/2023) define sua Política de Proteção de Dados Pessoais, aplicável a qualquer operação de tratamento de dados no Tribunal.

A Política visa garantir a proteção das informações e dos direitos dos titulares que estejam sob responsabilidade do STJ, os quais deverão ser mantidos de forma íntegra e confidencial, restringindo-se o tratamento em conformidade com a LGPD bem como às orientações dos órgãos de controle e reguladores.

Nos termos da Resolução, ainda, a presidência do STJ deverá criar o Comitê Gestor de Proteção de Dados Pessoais (CGPD). As funções do Comitê consistem em avaliar os mecanismos de tratamento e de proteção de dados pessoais já existentes no Tribunal, além de incentivar novas ações e boas práticas nos termos da lei.

TRT-SP: infração à LGPD é motivo para demissão por justa causa

A juíza da 81ª Vara do Trabalho de São Paulo (VT/SP) reconheceu a demissão por justa causa do enfermeiro que movia uma ação contra uma empresa administradora de hospitais por violação de diretrizes da LGPD.

O objeto da ação permeava o reconhecimento de rescisão indireta do contrato de trabalho, para que a demissão do trabalhador reclamante fosse convertida em dispensa sem justa causa. No decorrer do processo, entretanto, o reclamante juntou planilhas internas do hospital com dados sensíveis de saúde de pacientes.

Com essa ação, a juíza entendeu pela prática de violação à intimidade e à privacidade de terceiros – pessoas naturais clientes da empresa reclamada. Dessa forma, reconheceu que o reclamante infringiu a LGPD, utilizando dados sensíveis de forma ilícita. Além disso, a infração por parte do hospital também foi reconhecida, tendo em vista que a empresa era a responsável pela guarda dos dados sensíveis de seus clientes.

03

Autoridades



Vazamento de dados entra no ranking de reclamações dos PROCONs

O relatório de reclamações dos PROCONs do ano de 2022 trouxe algumas novidades, em especial para serviços na internet. Pela primeira vez, reclamações a respeito de provedores de aplicações ficaram entre os assuntos mais reclamados do ano no portal Consumidor.gov.br.

Segundo a Secretaria Nacional de Defesa do Consumidor (SENACON), as reclamações sobre os provedores de aplicação envolveram (i) a dificuldade de contato e a demora no atendimento oferecido; (ii) problemas para ativar e alterar serviços fornecidos por provedores de aplicação; e (iii) vazamento de dados pessoais e outros incidentes de segurança.

O vazamento de dados, apesar de não ter sido o assunto mais reclamado a respeito do setor, entrou pela primeira vez no ranking de reclamações, representando cerca de 15% das queixas dos consumidores.

Embora as empresas de tecnologia tenham sido incluídas no relatório de 2022, elas também são as com a maior capacidade de responder aos problemas indicados pelos clientes. A taxa de resolução das reclamações dos consumidores chega a quase 83%.

SENACON e ANPD prorrogam Acordo de Cooperação Técnica

Em 23 de março, foi publicado no Diário Oficial da União, o termo aditivo que prorroga o ACT entre a ANPD e a SENACON, no período de 22 de março de 2023 até 21 de março de 2025.

O acordo tem como objetivo principal o compartilhamento de informações coletadas envolvendo reclamações de consumidores no âmbito da proteção de dados pessoais. Prevê também, ações conjuntas nas áreas de defesa do consumidor, incluindo intercâmbio de informações, uniformização de entendimentos, cooperação em ações de fiscalização, desenvolvimento de ações de educação, formação e capacitação, além de elaboração de estudos e pesquisas. O acordo é parte do Planejamento Estratégico da ANPD para promover o fortalecimento da cultura de Proteção de Dados.

Com essa prorrogação, as duas entidades alinham esforços e reforçam as fiscalizações, de forma a garantir a proteção dos dados pessoais dos cidadãos brasileiros.

ANPD inicia julgamento de processos administrativos por violações à LGPD

A ANPD iniciou a análise dos primeiros oito processos administrativos relacionados a supostas violações à LGPD. A maior parte dos processos envolve órgãos do setor público federal e vazamentos de dados pessoais.

O regulamento de dosimetria e cálculo das penas publicado pela ANPD permite que a autarquia puna agentes do setor público e privado por violações à LGPD. As multas podem chegar a R\$ 50 milhões.

Além de sanções, a ANPD pode exigir a adoção de medidas corretivas para evitar novas infrações a titulares de dados. Segundo a diretora da ANPD, um segundo lote de processos envolverá empresas privadas, com situações que vão além de incidentes de segurança, como venda e compartilhamento de dados.

A ANPD concentrará seus esforços nos maiores agentes de tratamento de dados. Plataformas digitais, mídias sociais, comércio eletrônico, telecomunicações e setor público serão os principais alvos de fiscalização neste primeiro momento.

Para a ANPD, o objetivo é mais do que punição, mas chamar a atenção para a necessidade de estar adequado à lei e garantir segurança e proteção ao cidadão.

Ministério Público.

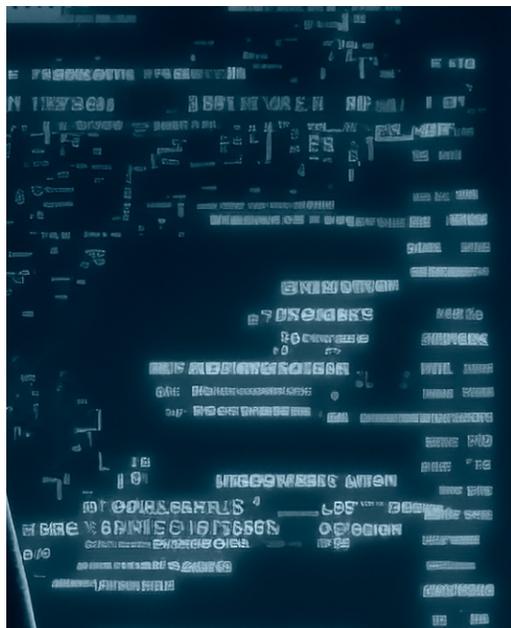
021

MPF publica relatório de atividades de proteção de dados pessoais

Diante dos novos desafios impostos pela LGPD, o Ministério Público Federal (MPF) instituiu um setor especializado para lidar com questões relacionadas a dados pessoais e criou a Unidade de Proteção de Dados Pessoais (UPDP). Vinculada ao gabinete do procurador-geral da República, a Unidade trabalha junto ao encarregado de Proteção de Dados Pessoais em atividades referentes a autodeterminação informativa do titular dos dados pessoais.

Com o Relatório de Atividades de 2022, a Unidade visa prestar contas e promover transparência das ações tomadas pela instituição e dos resultados alcançados.

O plano de ação já foi feito com delimitações em relação aos eixos de atuação, que englobam Governança, Conformidade, Transparência, Contratos e Segurança dos Dados. Também foram incluídas as previsões de atuação programadas para cada eixo para o período de junho de 2022 até junho de 2023, além de informações sobre reuniões e eventos.



05

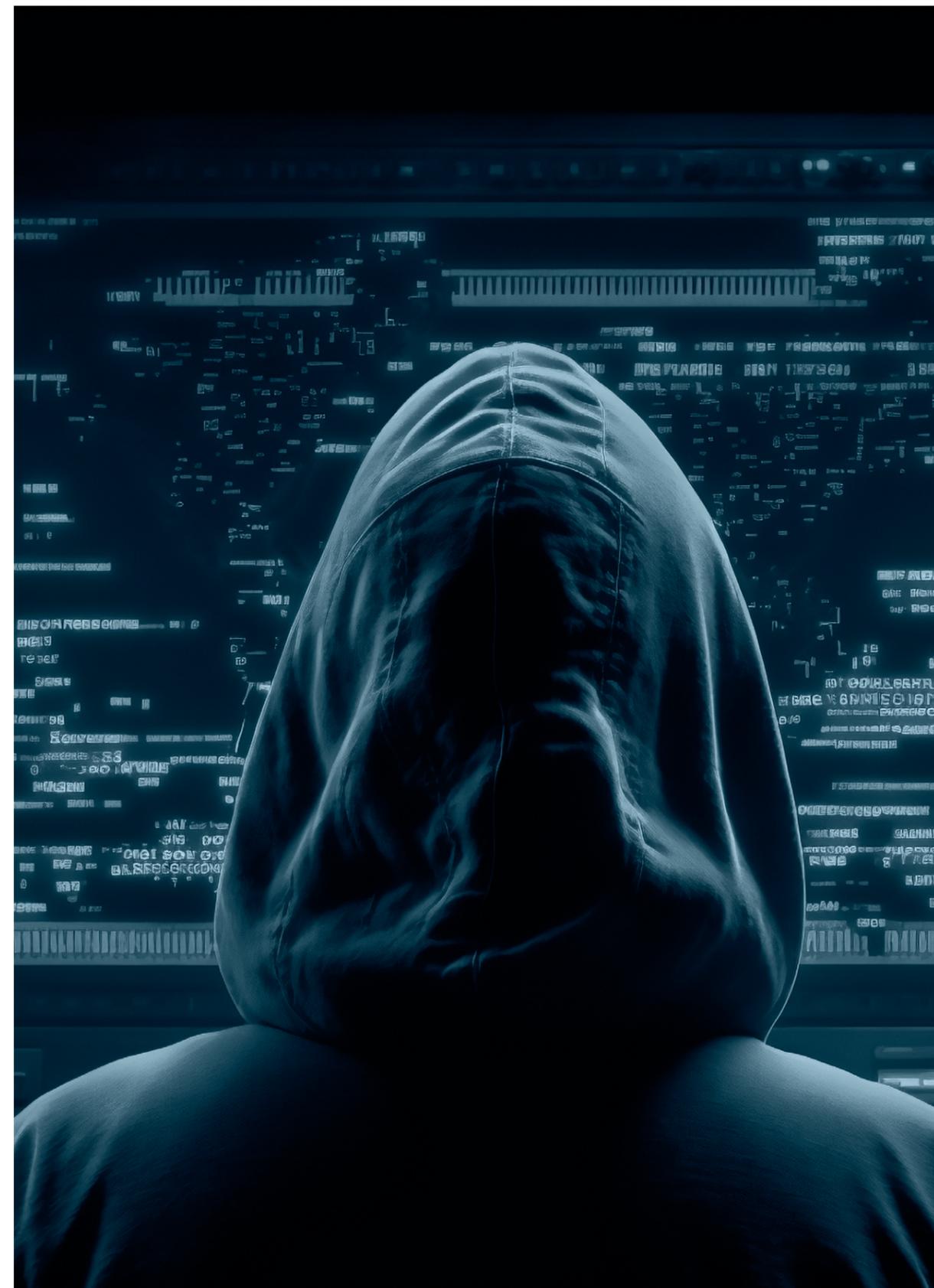
Avanços Normativos.

Convenção sobre o Crime Cibernético foi promulgada

Foi promulgada, em 13 de abril de 2023, a [Convenção sobre o Crime Cibernético](#), firmada pelo Brasil em Budapeste, na Hungria, em 23 de novembro de 2001. Atualmente, 66 nações são signatárias da Convenção, que busca a cooperação internacional para o combate de crimes praticados por meio da internet.

A Convenção parte de premissas como o impedimento de ações contra confidencialidade, integridade e disponibilidade de sistemas informáticos, redes e dados de computador, além do impedimento de abuso desses sistemas. Além disso, descreve diversos crimes cibernéticos, como acesso ilegal, violação de dados, interferência em sistemas e crimes relacionados ao conteúdo da informação.

A partir dessa promulgação, autoridades brasileiras contarão com maior facilidade para prosseguir com investigações de crimes que acontecem no ambiente virtual, especialmente aqueles que tenham provas de crimes obtidas no exterior. Da mesma forma, o Brasil se compromete a auxiliar as autoridades estrangeiras signatárias da Convenção.



06

Decisões Internacionais.

Comitê Europeu para a Proteção de Dados publica nova versão de suas diretrizes

Em 28 de março de 2023, o Comitê Europeu para a Proteção de Dados (EDPB, na sigla em inglês) publicou a segunda versão de suas [“Diretrizes 9/2022 sobre notificação de incidentes de segurança à luz do Regulamento Geral sobre a Proteção de Dados \(GDPR, na sigla em inglês\) da União Europeia”](#).

A fim de esclarecer quando um incidente de segurança deve ser comunicado, dentro do Espaço Econômico Europeu (EEE), às autoridades de proteção de dados ou aos titulares afetados, as Diretrizes trazem à tona parâmetros para determinar o grau de risco de determinado incidente que tenha identificado ou tomado conhecimento. A medida levará à necessidade ou não de notificar a Autoridade europeia competente e os titulares afetados.

Nesse contexto, o EDPB reconhece que a avaliação do “risco aos direitos e liberdades dos titulares” deve considerar critérios tais como:

- o tipo do incidente,
- a natureza, volume e sensibilidade dos dados afetados,
- a facilidade de identificação dos titulares cujos dados foram envolvidos no incidente,
- suas consequências concretas (como o potencial de causar em falsificação de identidade, danos físicos, angústia psicológica, humilhação ou dano reputacional),
- a potencial vulnerabilidade do titular,
- o grau de risco do tipo de atividade desenvolvida pelo agente de tratamento e
- o número de titulares afetados.

Com esses parâmetros em perspectiva, se identificado o potencial de risco aos titulares, as Autoridades europeias de proteção de dados deverão ser notificadas (assim como os próprios titulares afetados caso o risco em questão seja alto). Ainda, as Diretrizes esclarecem que agentes de tratamento deverão reportar o incidente para a Autoridade de cada país no EEE em que tiverem sido identificados titulares afetados.

ChatGPT é banido temporariamente na Itália e investigado por autoridade canadense

A plataforma de geração de textos por meio de inteligência artificial foi temporariamente banida de operar na Itália. O ChatGPT também foi alvo de investigação no Canadá, entre o final de março e o início de abril. Há preocupação, entre as autoridades de proteção de dados dos países, de que dados pessoais de titulares estejam sendo tratados sem o devido consentimento.

Além do banimento temporário, a autoridade italiana disse preparar uma investigação para averiguar se a OpenAI, empresa responsável pelo ChatGPT, opera em conformidade com o GDPR. A autoridade canadense, porém, não revelou mais detalhes sobre a investigação em curso.

Ainda, a autoridade italiana colocou prazo para a OpenAI explicar como serão abordados os pontos levantados pela autoridade, sob pena de multas de até EUR 20 milhões ou até 4% da receita anual da empresa.

Em 13 de abril de 2023, durante uma reunião do EDPB, também foi decidido que uma força-tarefa conjunta será lançada para discutir questões envolvendo proteção de dados e o ChatGPT.

487095484

265873282

```
age = ATOMIC_INIT(2) );  
dsetsize){
```

```
struct group_info init_groups = { .usage = ATOMIC_INIT(2) };  
struct group_info *groups_alloc(int gidsetsize){  
struct group_info *group_info;  
376984373  
last one indirect block pointer */int nblocks)
```

Este boletim é um informativo da área
de Cybersecurity & Data Privacy de
TozziniFreire Advogados.

**SÓCIAS RESPONSÁVEIS
PELO BOLETIM:**

Marcela Waksman Ejnisman

-  Patrícia Helena Marta Martins
-  Carla do Couto Hellu Battilana
-  Bruna Borghi Tomé
-  Luiza Sato
-  Sofia Kilmar

Mais informações em:

tozzinifreire.com.br

**Tozzini
Freire.**
ADVOGADOS

821439828

```
struct group_info init_groups = { .usage = ATOMIC_INIT(2) };  
struct group_info *groups_alloc(int gidsetsize){
```